Wireless
Network Security

Alec Yasinsac
SAIT Laboratory
Florida State University

Quote of the Day

Focus on the Long Term

- "Winston, you are drunk!"

  – Lady Astor

- "Yes my dear, and you are ugly.
  In the morning I shall be sober."

  – Winston Churchill

Wireless Security Issues

- Overview
- Static Access Points
  - –IEEE 802.1x
- Ad hoc Networks
  - –Conference Key Generation & Distribution
  - –Secure Routing Protocols

Wireless Security Issues

- **Overview**
- Static Access Points
  - –IEEE 802.1x
- Ad hoc Networks
  - –Conference Key Generation & Distribution
  - –Secure Routing Protocols

Wireless Complicators

1. Broadcast
2. Dynamic Nature

Communication Issues

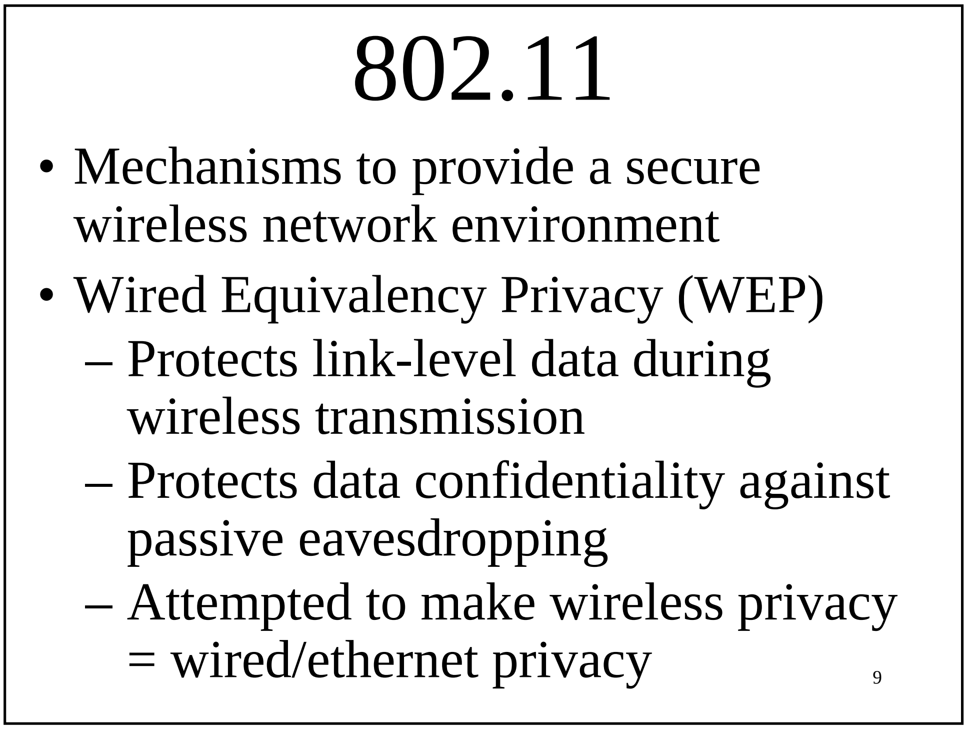
- Broadcast paradigm
- Bandwidth is limited
- Distance limited
- Line of sight matters
- Power consumption
- Etc.

Wireless Security Issues

- Overview
- Static Access Points
  - –IEEE 802.1x
- Ad hoc Networks
  - –Conference Key Generation & Distribution
  - –Secure Routing Protocols

Static Access Points

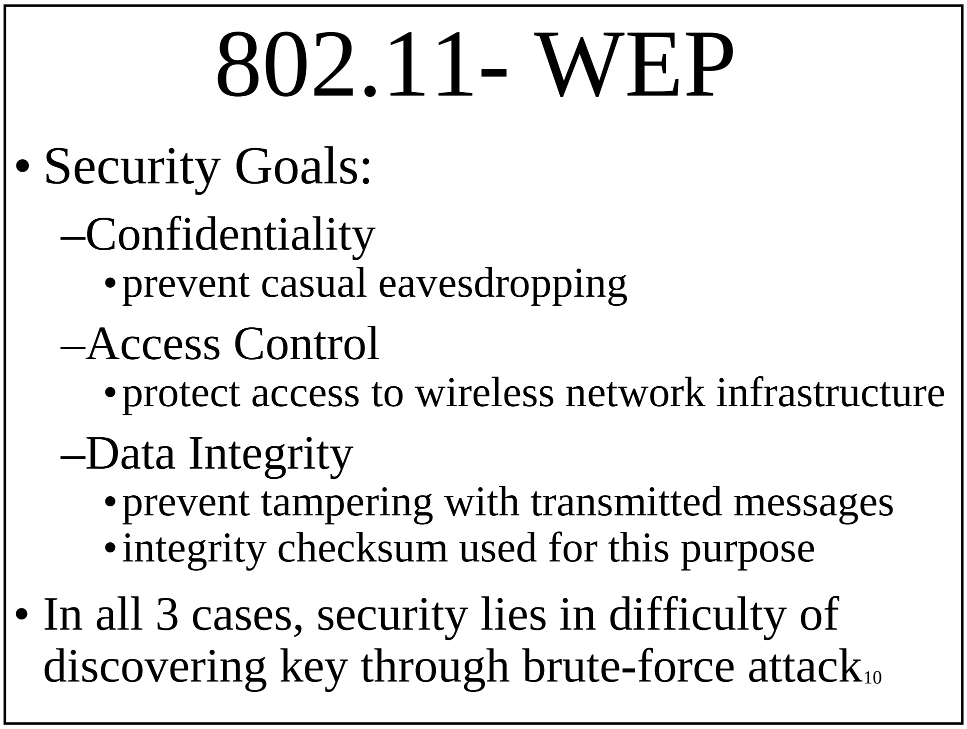
- Communications of the ACM, May 2003
- Overview
- 802.11
  - –The Good
  - –The Bad (it is ugly)



802.11

- Mechanisms to provide a secure wireless network environment
- Wired Equivalency Privacy (WEP)
  - Protects link-level data during wireless transmission
  - Protects data confidentiality against passive eavesdropping
  - Attempted to make wireless privacy = wired/ethernet privacy

9



802.11- WEP

- Security Goals:
  - Confidentiality
    - prevent casual eavesdropping
  - Access Control
    - protect access to wireless network infrastructure
  - Data Integrity
    - prevent tampering with transmitted messages
    - integrity checksum used for this purpose
- In all 3 cases, security lies in difficulty of discovering key through brute-force attack

10

802.11 Modes

- Works in two modes:
  - Ad-hoc mode
    - Independent Basic Service Set (IBSS)
    - Client communicates directly with other clients
    - Only clients within transmission range (cell) of each other can communicate
  - Infrastructure mode
    - Basic Service Set (BSS)
    - Client communicates with central station which forwards communication

802.11 Modes

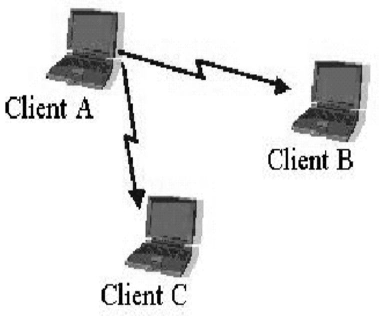


Figure 2: Example ad-hoc network

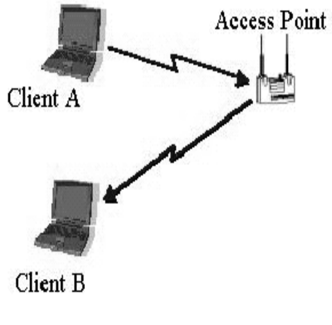
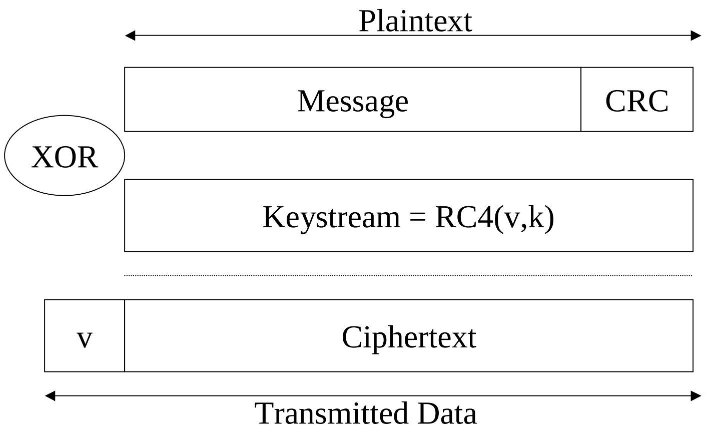


Figure 3: Example infrastructure network

802.11- WEP

- WEP relies on a secret key k
  - shared between communicating parties
  - used to protect body of transmitted frame of data

802.11-WEP Picture



Plaintext

Message

CRC

XOR

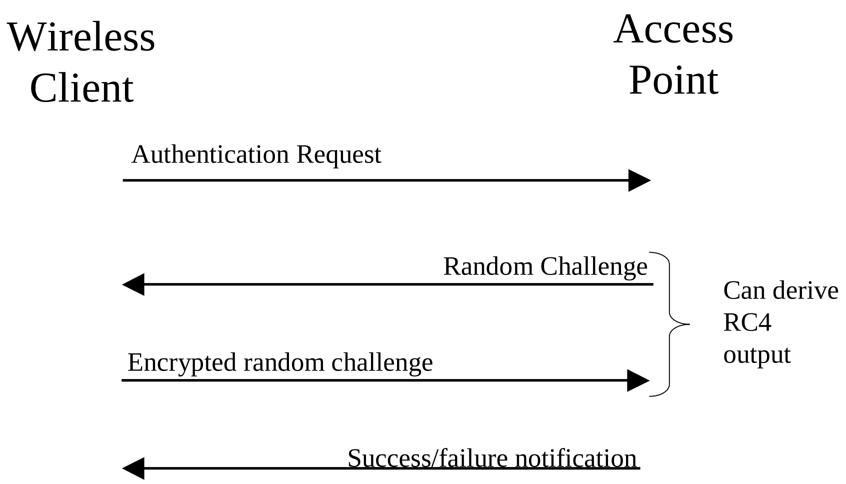
Keystream = RC4(v,k)

v

Ciphertext

Transmitted Data

WEP Authentication



Wireless Client

Access Point

Authentication Request

Random Challenge

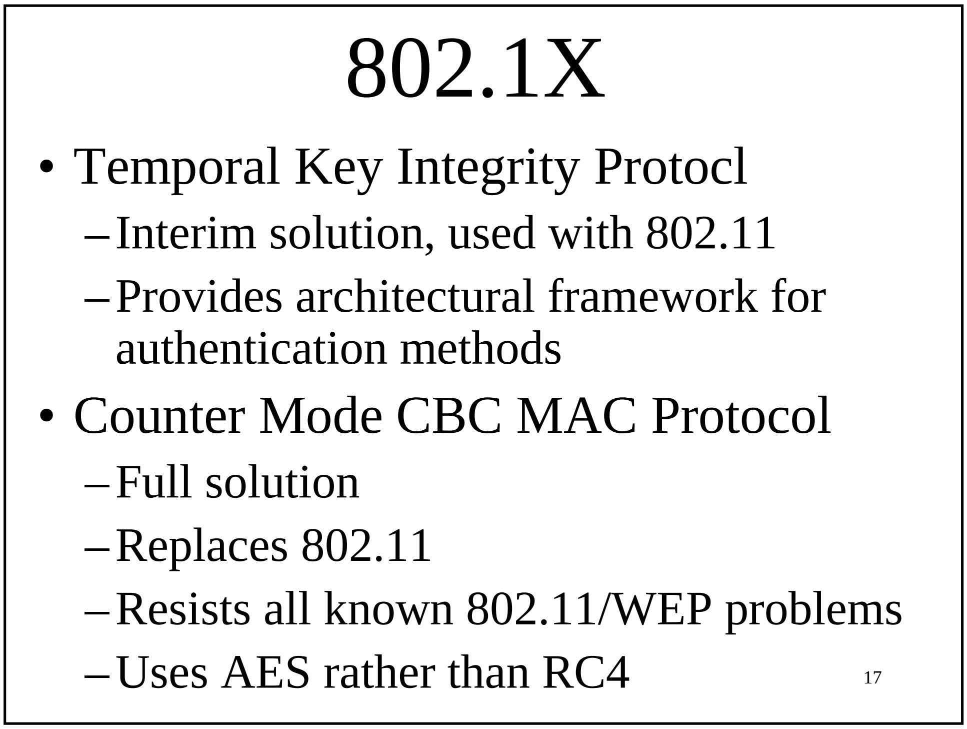
Encrypted random challenge

Can derive RC4 output

Success/failure notification

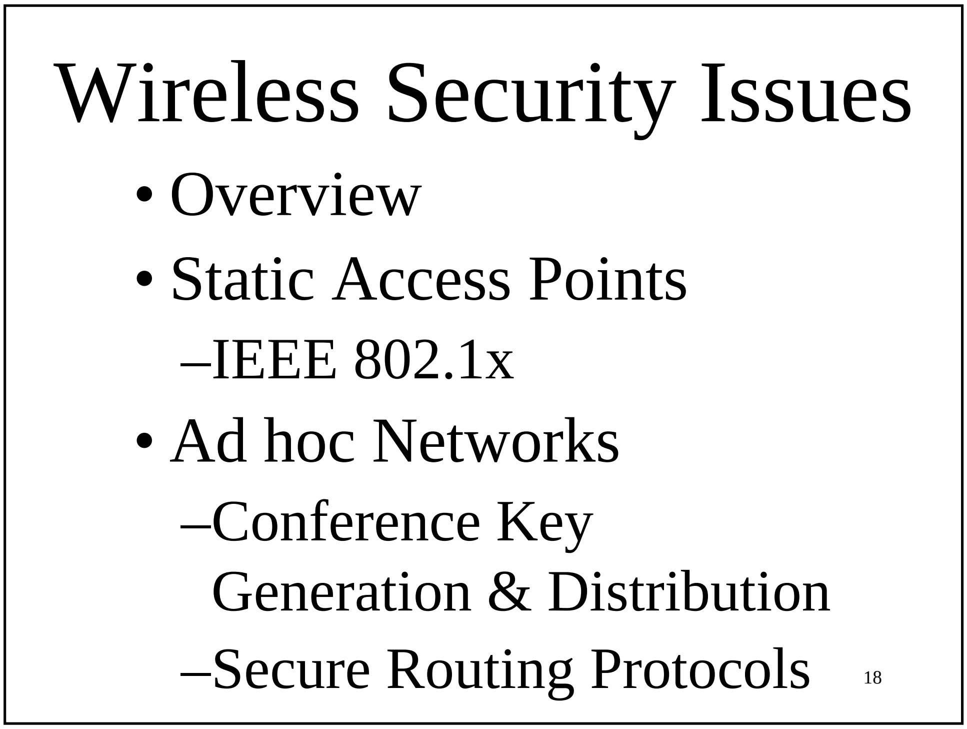
802.11 Effectiveness

- None of the 3 security goals attained
  - –Practical attacks allow eavesdropping
  - –It is possible to subvert the integrity checksum field (modify messages)
  - –New traffic can be injected into the network



802.1X

- Temporal Key Integrity Protocl
  - Interim solution, used with 802.11
  - Provides architectural framework for authentication methods
- Counter Mode CBC MAC Protocol
  - Full solution
  - Replaces 802.11
  - Resists all known 802.11/WEP problems
  - Uses AES rather than RC4



Wireless Security Issues

- Overview
- Static Access Points
  - IEEE 802.1x
- Ad hoc Networks
  - Conference Key Generation & Distribution
  - Secure Routing Protocols

The Essence of:

- Ad hoc
  - Dynamic
  - Unpredictable
  - No controlling authority
  - No structure
- Function
  - Action with a purpose
  - Predictable
  - Reliable
  - Static

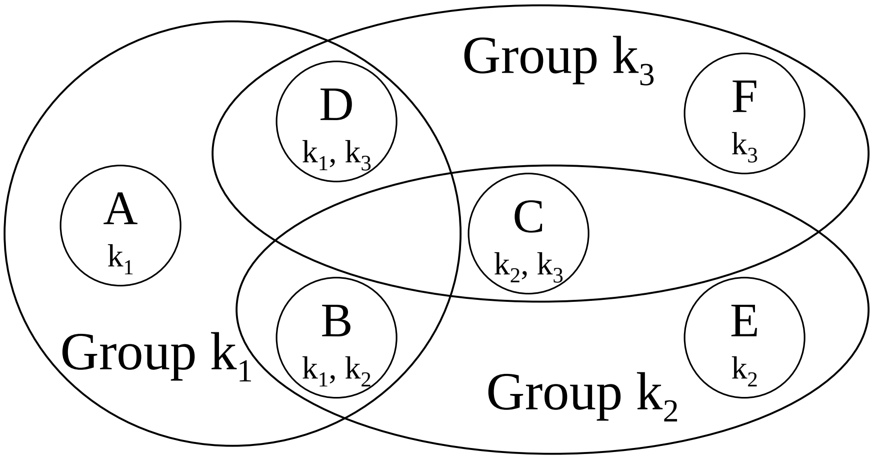
Keys in Group Communication

- Generate New Keys
- Distribute New Keys
- Distribute Old Keys
- Change Keys
- Revoke Keys

Secure Group Communication

- Guarantee Inclusiveness
  - –Ensure delivery to all intended recipients
  - –Technology: Communications
- Guarantee Exclusiveness
  - –Restrict delivery to only intended recipients
  - –Technology: Cryptography

Group Keys



Secure Groups in Ad hoc Networks

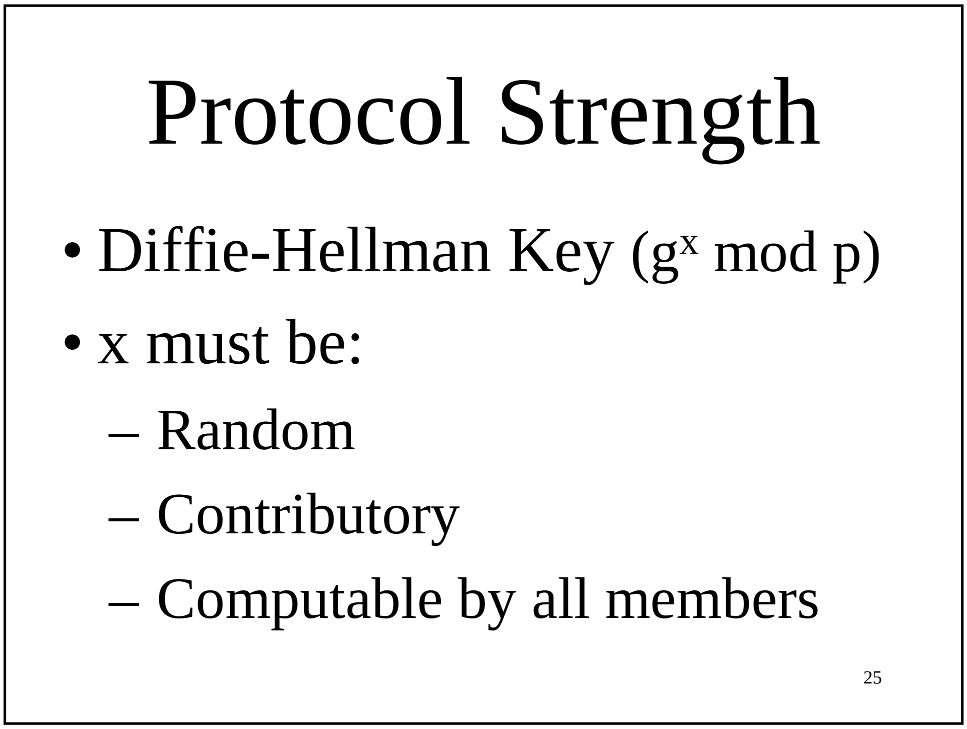
- Cryptographic protocols
- Requirements
  - –Distributed
  - –Efficient
  - –Contributory

No Structure Required

Existing Protocols

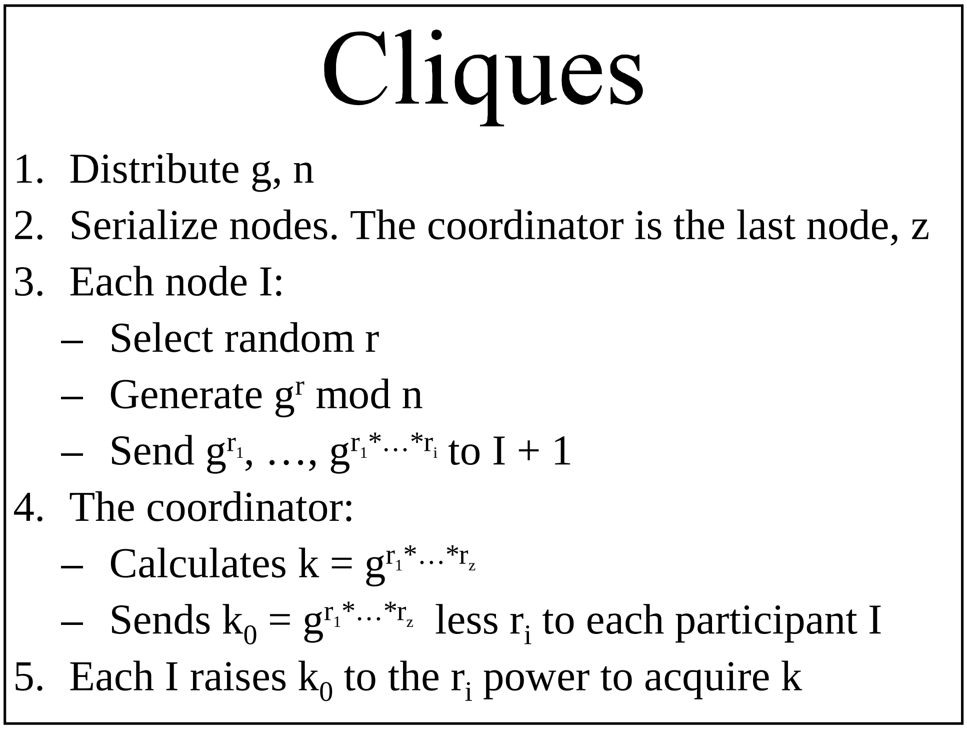
- Burmester/Desmedt (1997)
- Cliques (1996-2000)

Require extensive, à priori network structure knowledge



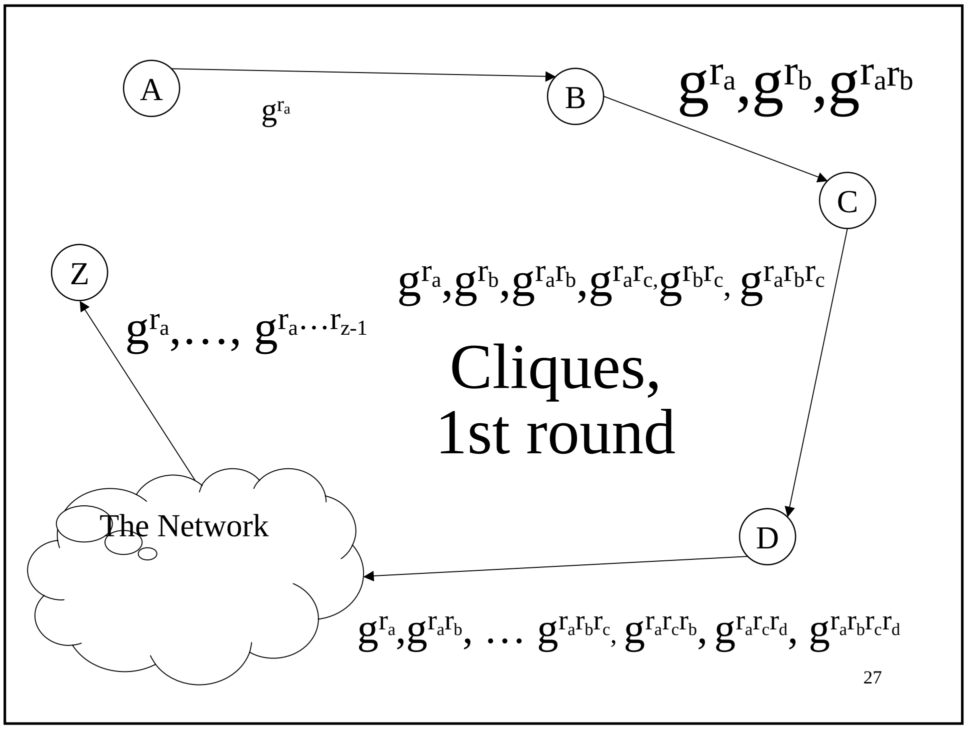
Protocol Strength

- Diffie-Hellman Key (g^x mod p)
- x must be:
  - Random
  - Contributory
  - Computable by all members



Cliques

1. Distribute g, n
2. Serialize nodes. The coordinator is the last node, z
3. Each node I:
   - Select random r
   - Generate g^r mod n
   - Send $g^{r_1}, \ldots, g^{r_1*\ldots*r_i}$ to I + 1
4. The coordinator:
   - Calculates $k = g^{r_1*\ldots*r_z}$
   - Sends $k_0 = g^{r_1*\ldots*r_z}$ less r_i to each participant I
5. Each I raises k_0 to the r_i power to acquire k



g^{r_a}

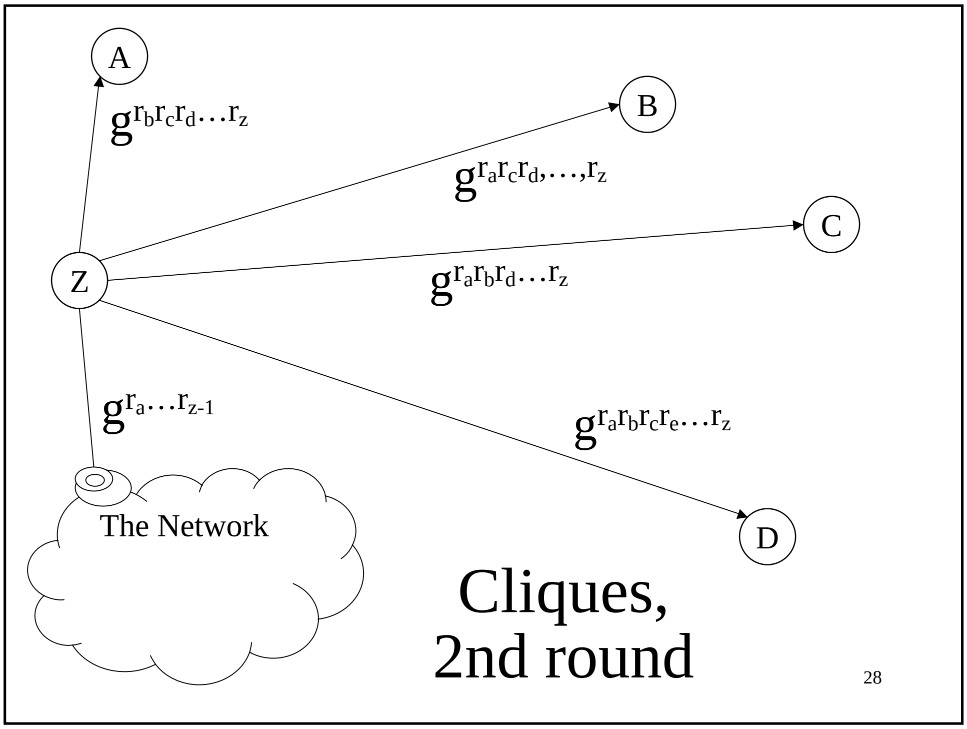
$g^{r_a}, g^{r_b}, g^{r_a r_b}$

$g^{r_a}, g^{r_b}, g^{r_a r_b}, g^{r_a r_c}, g^{r_b r_c}, g^{r_a r_b r_c}$

$g^{r_a}, \ldots, g^{r_a \ldots r_{z-1}}$

Cliques,
1st round

$g^{r_a}, g^{r_a r_b}, \ldots\ g^{r_a r_b r_c}, g^{r_a r_c r_b}, g^{r_a r_c r_d}, g^{r_a r_b r_c r_d}$



$g^{r_b r_c r_d \ldots r_z}$

$g^{r_a r_c r_d, \ldots, r_z}$

$g^{r_a r_b r_d \ldots r_z}$

$g^{r_a \ldots r_{z-1}}$

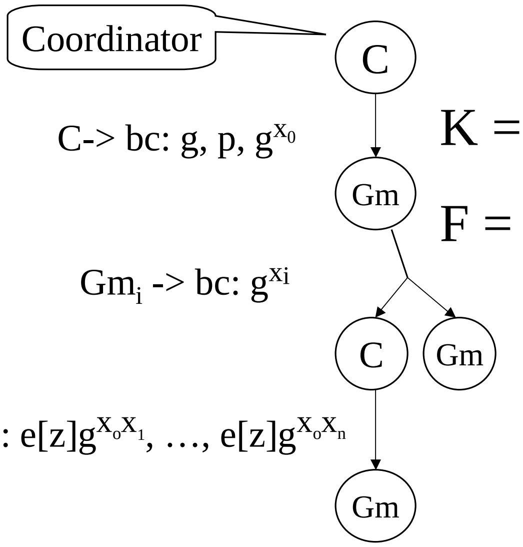
$g^{r_a r_b r_c r_e \ldots r_z}$

Cliques,
2nd round

Problems With Cliques

1. Serialization requirement
2. Number of computations
3. Size of messages

Leveraging Broadcast
An Optimal Contributory Protocol



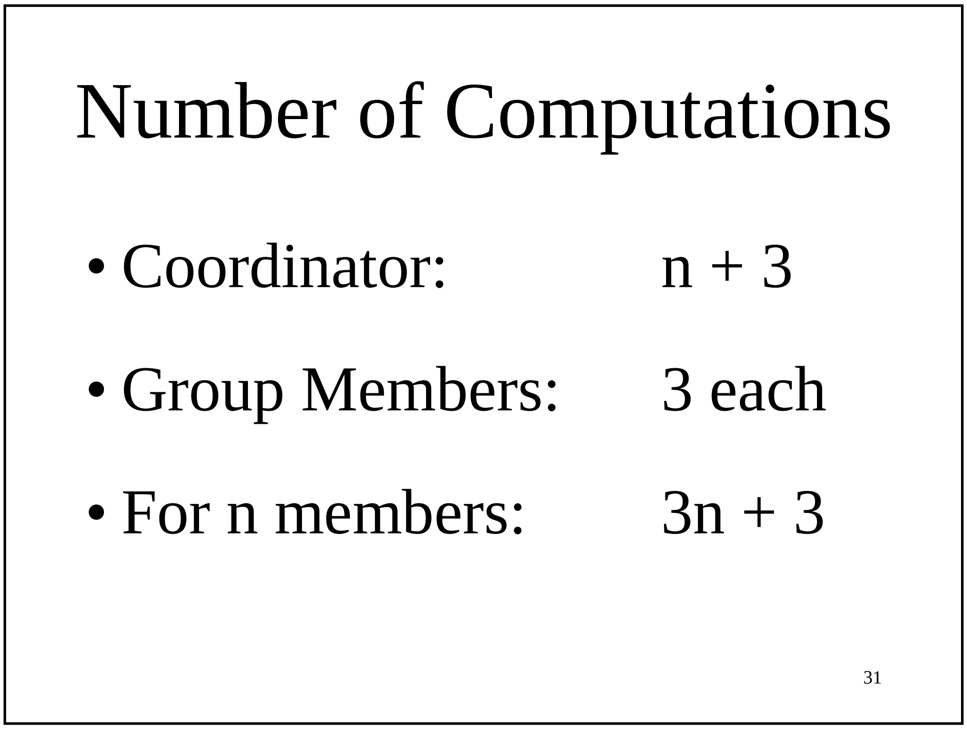
C-> bc: g, p, g^{x_0}

Gm$_i$ -> bc: g^{x_i}

C-> bc: $e[z]g^{x_o x_1}$, …, $e[z]g^{x_o x_n}$

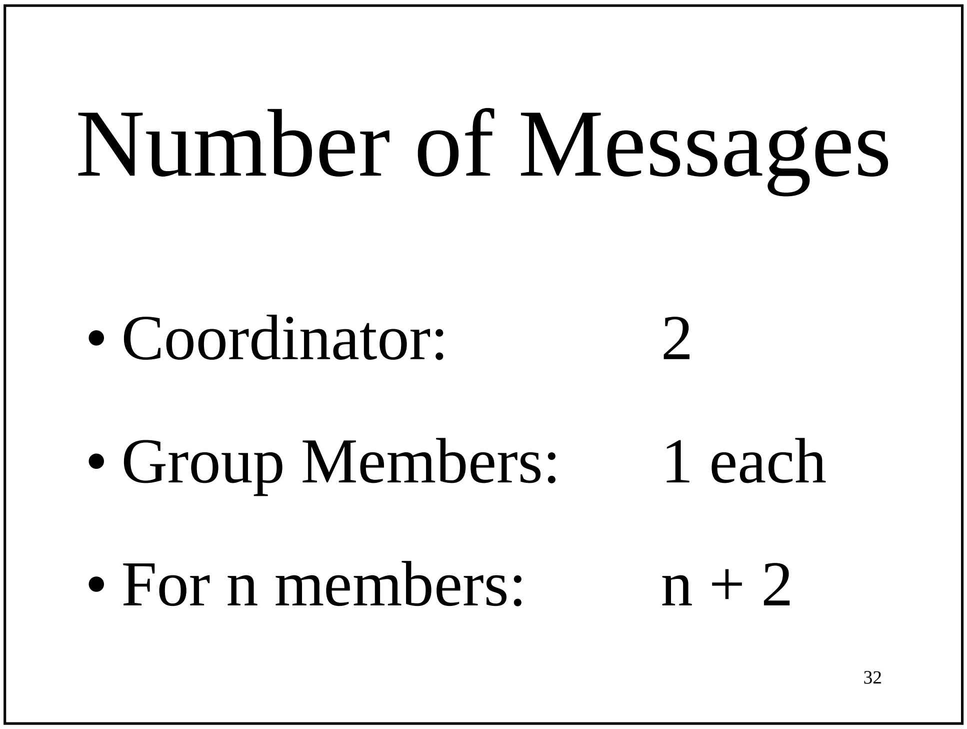
$K = g^{F}\ \ z$, where

$F = f(g^{x_1}, ..., g^{x_n})$



Number of Computations

- Coordinator: n + 3
- Group Members: 3 each
- For n members: 3n + 3



Number of Messages

- Coordinator: 2
- Group Members: 1 each
- For n members: n + 2

Size of Messages

• Coordinator:	1 large, 1 small
• Group Members:	1 small each
• For n members:	1 large, n small

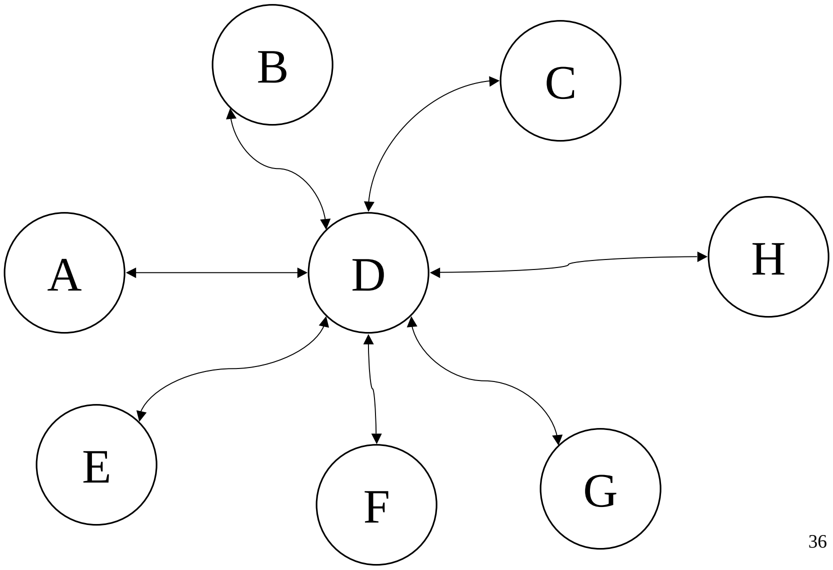
Wireless Security Issues

- Overview
- Static Access Points
  - IEEE 802.1x
- Ad hoc Networks
  - Conference Key Generation & Distribution
  - Secure Routing Protocols

Routing Defined

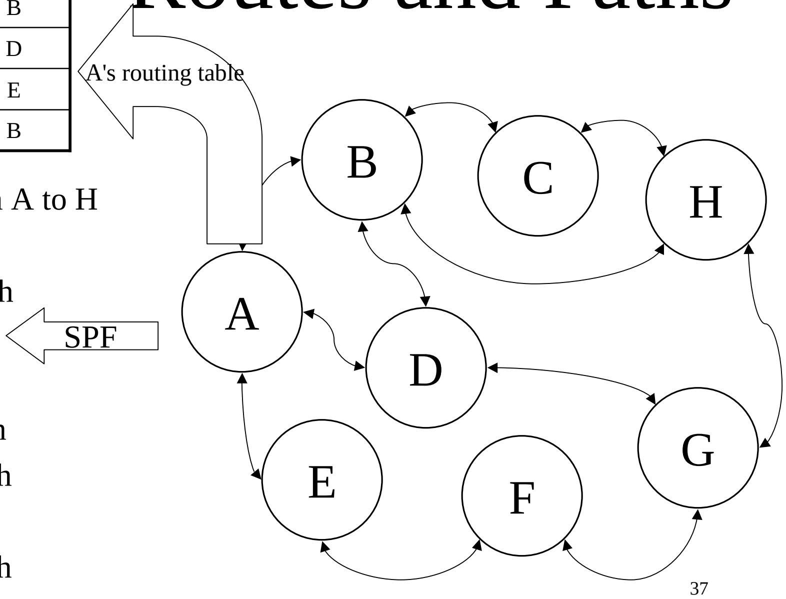
- Macro
  - –Finding the optimal path between nodes in a network
- Micro
  - –Algorithm to decide which interface to relay each message
  - –Options: None, all, selected

Easy Routing



Routes and Paths

Destination	Interface
C	B
G	D
F	E
H	B



- Paths from A to H
  1. abch
  2. abdgh
  3. abh
  4. adgh
  5. aefgh
  6. adbch
  7. adbh
  8. agcgh
  9. etc.

Goals of Routing

Reliably and efficiently establish a relay path between sender and receiver

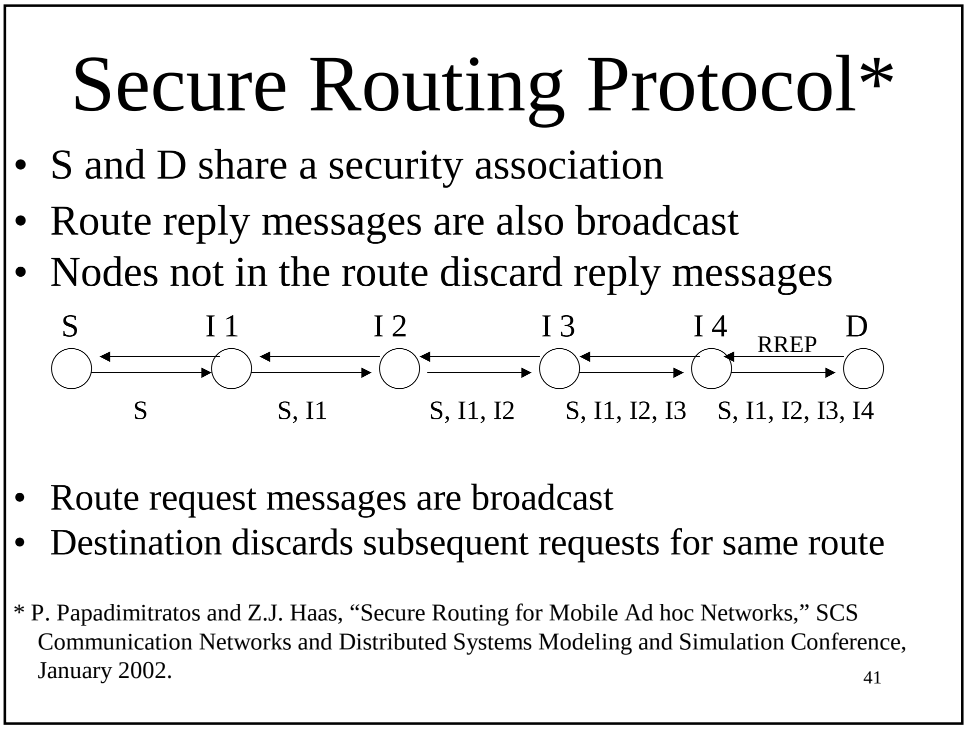
- Reliability
  - Guarantee/Optimize/Verify delivery
  - Load balancing, other net mgmt
- Efficiency, optimize:
  - Number of messages
  - Number of links
  - Time
  - Etc.

Secure Routing Goal

1. Protect routing information
   - Routing Tables
   - Route Maintenance Data in Transit

Secure Routing Goals

1. Fabricated routing messages cannot be injected
2. Routing messages cannot be altered in transit
3. Routing loops cannot be maliciously inserted
4. Routes cannot be redirected from shortest path
5. Unauthorized nodes are excluded from routes
6. Network topology must not be exposed to malicious nodes via routing messages
7. Nodes must not store inaccurate routing data



Secure Routing Protocol*

- S and D share a security association
- Route reply messages are also broadcast
- Nodes not in the route discard reply messages

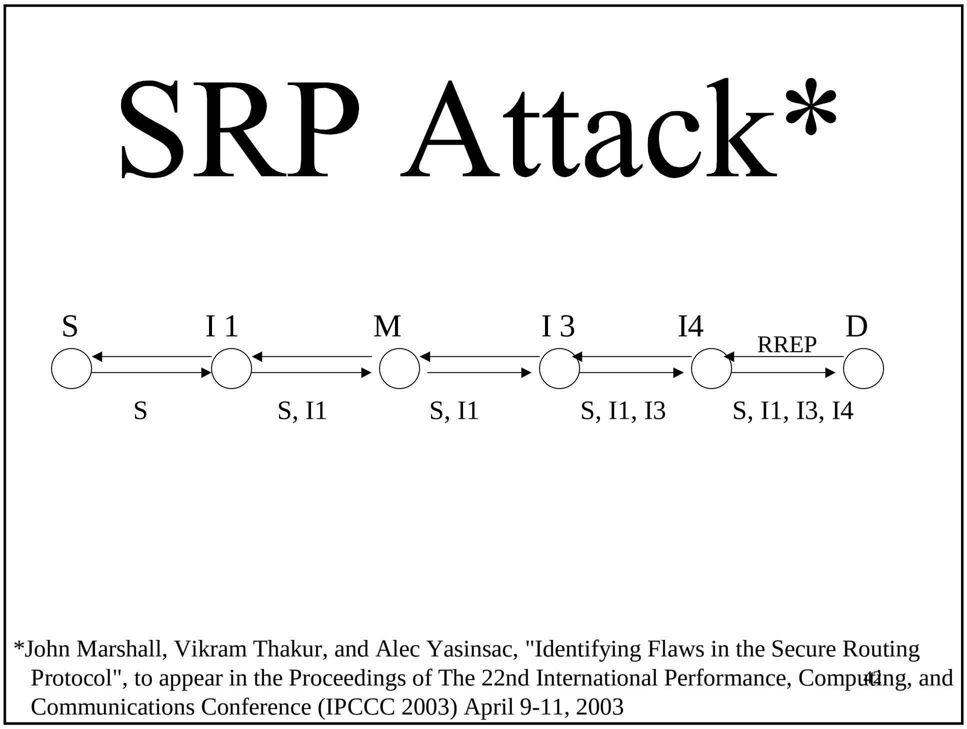
S I 1 I 2 I 3 I 4 D

RREP

S | S, I1 | S, I1, I2 | S, I1, I2, I3 | S, I1, I2, I3, I4

- Route request messages are broadcast
- Destination discards subsequent requests for same route

* P. Papadimitratos and Z.J. Haas, “Secure Routing for Mobile Ad hoc Networks,” SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, January 2002.



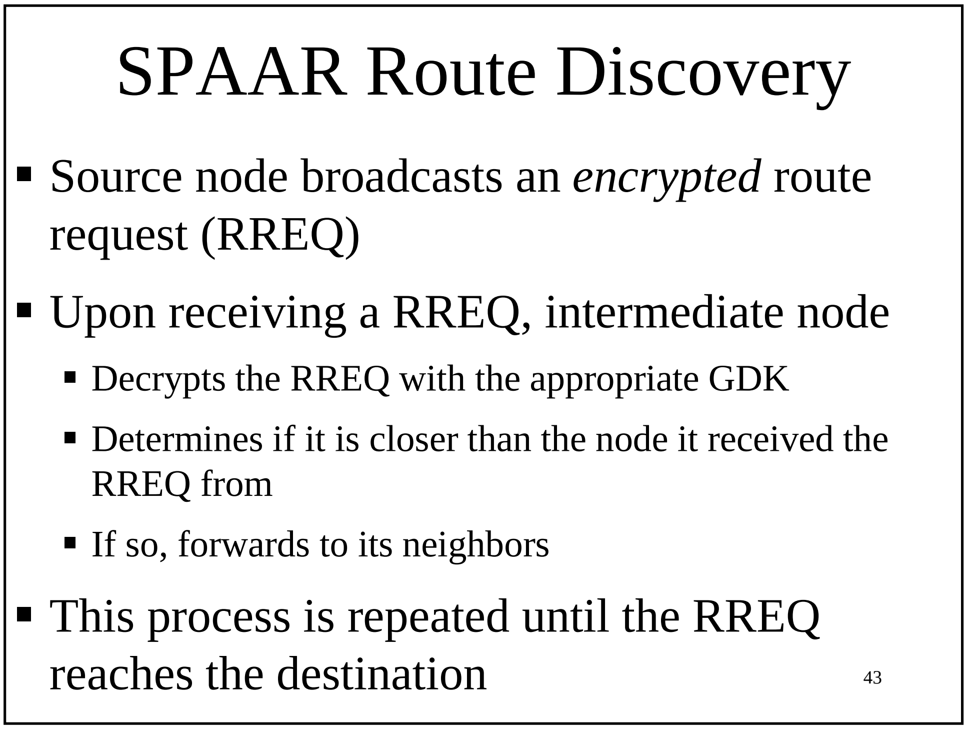
SRP Attack*

S I 1 M I 3 I4 D

RREP

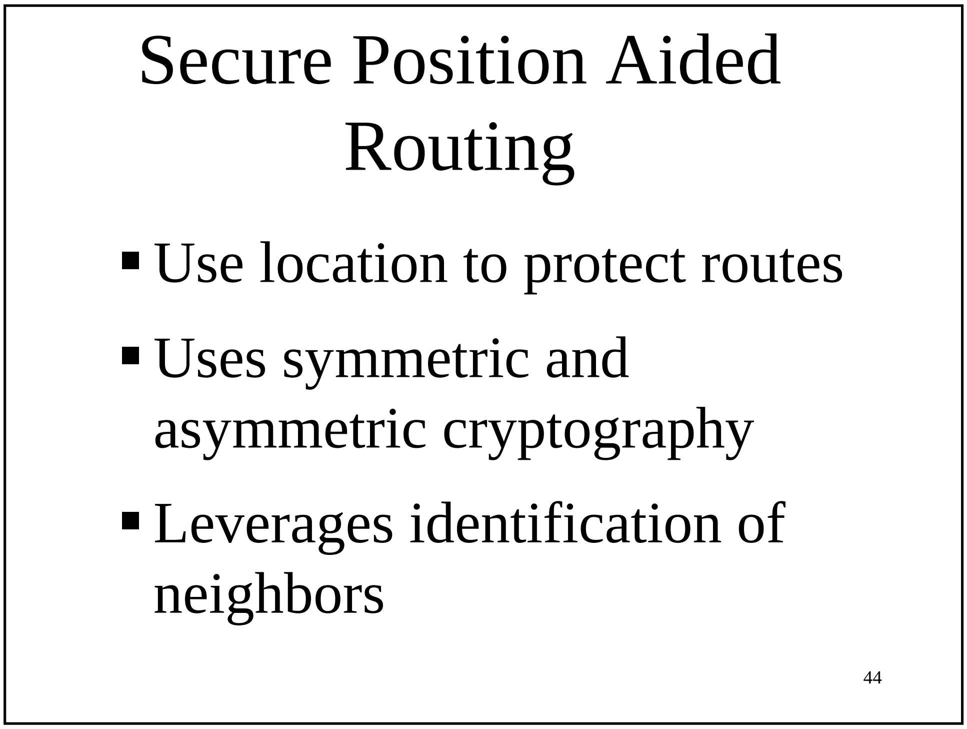
S | S, I1 | S, I1 | S, I1, I3 | S, I1, I3, I4

*John Marshall, Vikram Thakur, and Alec Yasinsac, "Identifying Flaws in the Secure Routing Protocol", to appear in the Proceedings of The 22nd International Performance, Computing, and Communications Conference (IPCCC 2003) April 9-11, 2003



SPAAR Route Discovery

- Source node broadcasts an *encrypted* route request (RREQ)
- Upon receiving a RREQ, intermediate node
  - Decrypts the RREQ with the appropriate GDK
  - Determines if it is closer than the node it received the RREQ from
  - If so, forwards to its neighbors
- This process is repeated until the RREQ reaches the destination



Secure Position Aided Routing

- Use location to protect routes
- Uses symmetric and asymmetric cryptography
- Leverages identification of neighbors

Location Aided Routing

- The use of position information can reduce overhead of the route discovery process
- Current position aided routing protocols are insecure because they pass location information in the clear

45

SPAAR Details

- Main components of SPAAR:
  - The Neighbor Table
    - Neighbor Discovery, Neighbor Table Maintenance
  - The Route Table
    - Route Discovery, Route Table Maintenance

46

SPAAR Setup

- Each node requires:
  - Public/Private key pair
  - Certificate binding identity to its public key
  - Public key of the trusted certificate server
- Each node must have access to a trusted certificate server at some time *prior* to deployment

The Neighbor Table

- Nodes maintain a neighbor table containing:
  - Neighbor ID
  - Neighbor’s Public Key
  - Neighbor’s Group Decryption key (GDK)
  - Most Recent Location (MRL)
  - Transmission Range (TR)
  - Location Update Sequence Number (LUSN)

Neighbor Table Setup

Each node generates a public/private key pair called the Neighbor Group Key Pair

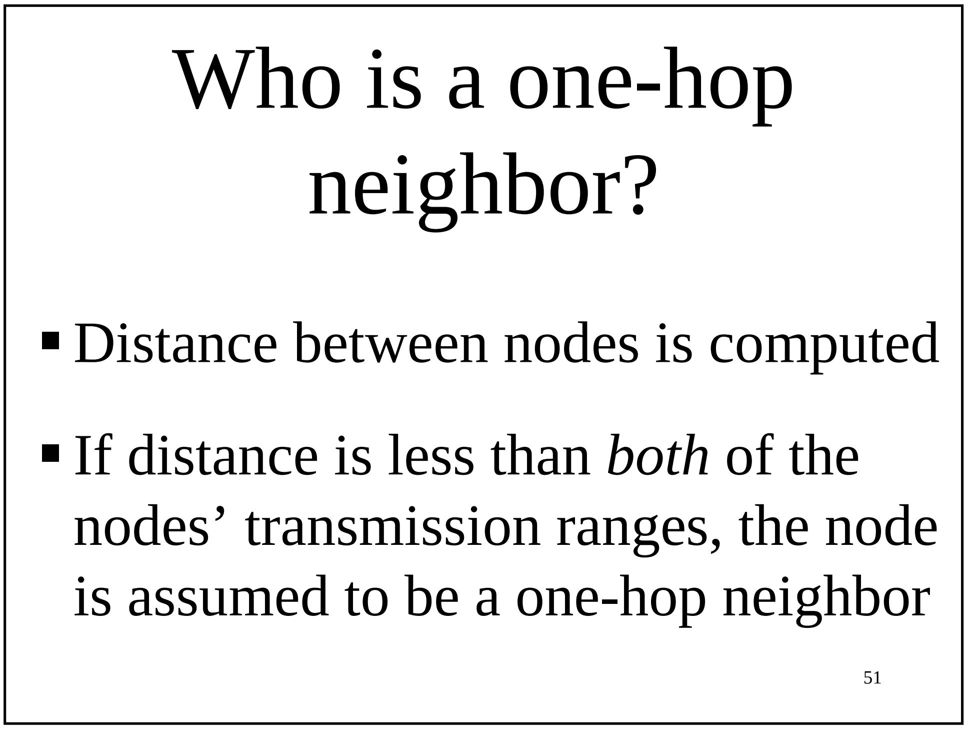
- The private part is called the ***group encryption key*** (GEK)
- The public part is called the ***group decryption key*** (GDK)

Adding nodes to the Neighbor Table

Step 1: A node N periodically broadcasts a “hello” message

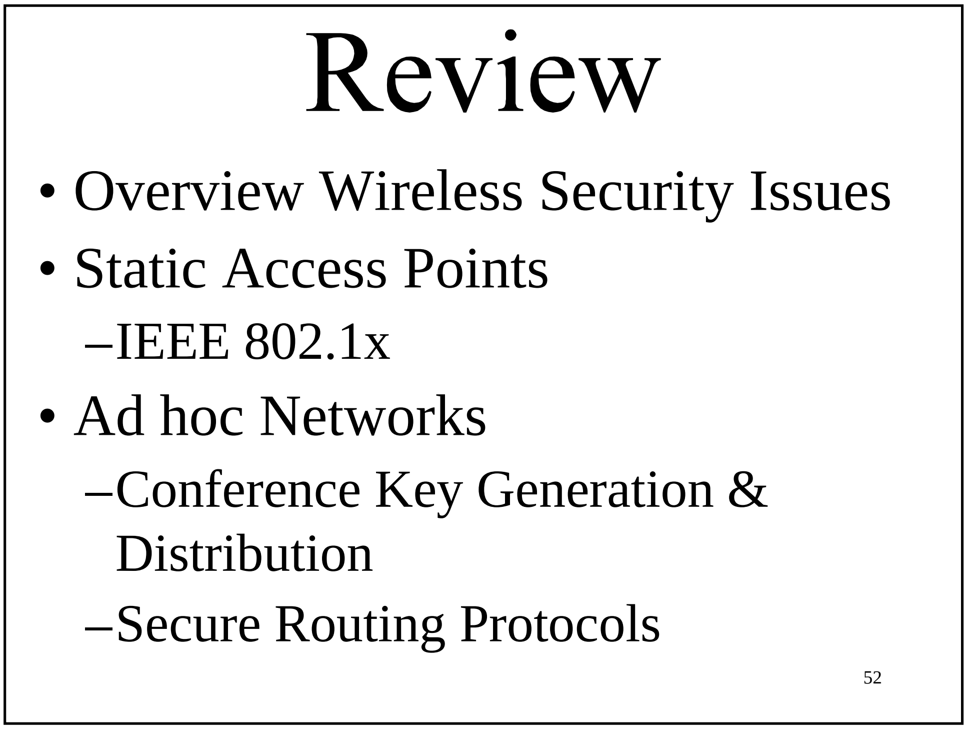
Step 2: Nodes within range respond with a “hello_reply”

Step 3: N distributes its GDK to each verified one hop neighbor



Who is a one-hop neighbor?

- Distance between nodes is computed
- If distance is less than *both* of the nodes’ transmission ranges, the node is assumed to be a one-hop neighbor



Review

- Overview Wireless Security Issues
- Static Access Points
  - IEEE 802.1x
- Ad hoc Networks
  - Conference Key Generation & Distribution
  - Secure Routing Protocols